Using the MIITS-Internet Tool to Perform Criticality Analysis of National Internet Infrastructure

Guanhua Yan, CCS-3; Pallab Datta, Neurosciences Institute; Stephan Eidenbenz, Sunil Thulasidasan, CCS-3; Venkatesh Ramaswamy, Airvana, Inc.

As the Internet has permeated into almost every aspect of our daily lives, it is of crucial importance to ensure that its critical infrastructure functions properly. The Internet infrastructure can suffer severe physical damages due to disastrous natural catastrophes, such as hurricanes and earthquakes, or some physical attacks. Meanwhile, a malicious cyber attack (e.g., a distributed denial-of-service attack) can cause undesirable effects if it completely disables a critical Internet infrastructure facility, or even only makes it behave abnormally. As many other infrastructures such as power grids and transportation systems become increasingly dependent on the Internet for their normal operations, it is vital to protect the critical Internet infrastructure from severe physical damages and malicious cyber attacks.

Given the vast scale of the Internet, it is a challenging task to decide where we should dedicate our resources to protect its infrastructure, especially when the provided resources are limited. To tackle this challenge, we extended the capabilities of the LANL-developed modeling and simulation suite MultiScale Integrated Information and Telecommunications System (MIITS), and with this MIITS-Internet tool, we performed criticality analyses of the Internet infrastructure at a national level from three different methodological perspectives. A *graph-theoretical analysis* studies the structural properties of a geographical network condensed from the Internet backbone topology, including its degree of distribution, clustering structure, and its centrality measures. Although theoretically appealing, graph-theoretical analysis ignores the hierarchical routing scheme of the real Internet and uses the shortest-path routing scheme due to its simplicity. *Route-based analysis*, instead, models realistic inter- and intradomain routing schemes used in the Internet and then identifies those facilities that appear most frequently on paths in the Internet backbone topology. Realizing that route-based analysis still produces biased results because all paths are evenly weighted, we propose another approach, traffic-based analysis, which weighs each path only by its traffic demands. To do this, we generate synthetic end devices and also session-level traffic among them. Different from previous efforts on Internet modeling, our work endeavors to achieve high fidelity by using realistic datasets such as U.S. census data, computer usage statistics, and market shares of Internet service providers.

Using the high-fidelity network model we have built, we find that the average number of locations each byte of domestic network traffic travels in the Internet backbone topology is about five—more specifically, the frequency histogram of the number of locations that a byte of domestic traffic visits in the Internet backbone is illustrated in Fig. 1. Furthermore, we rank different locations in the backbone based on the amount of traffic that travels through them and show the result in Fig. 2. We note that the top location is traversed by about 70 percent of the total traffic. Although surprising, this result is actually in concert with earlier observations that some locations witness more than 50 percent of the Internet traffic in the U.S. [1,2].

In a nutshell, the key findings with the MIITS-Internet tool include the following.

(1) The geographical topology, which is condensed from a national-level IP backbone network and has a power-law degree distribution—it is a small-world network with a high clustering coefficient and a small characteristic path length. Moreover, the number of IP addresses at each location in the IP backbone network is well characterized by a power-law distribution.

(2) A few locations appear much more frequently than others among all paths in the IP backbone topology, and these locations also witness a high percentage of the Internet traffic in the whole US.

(3) Relative ranks of Internet facility locations from traffic-based analysis differ significantly from those derived from graph-theoretical analysis and route-based analysis, suggesting that a comprehensive, high-fidelity Internet model is necessary to assess critical Internet infrastructure facilities.

For further information contact Guanhua Yan at ghyan@lanl.gov.

[1] http://www.usipv6.com/6sense/2005/sep/03.htm
[2] http://www.foxnews.com/story/0,2933,347035,00.html

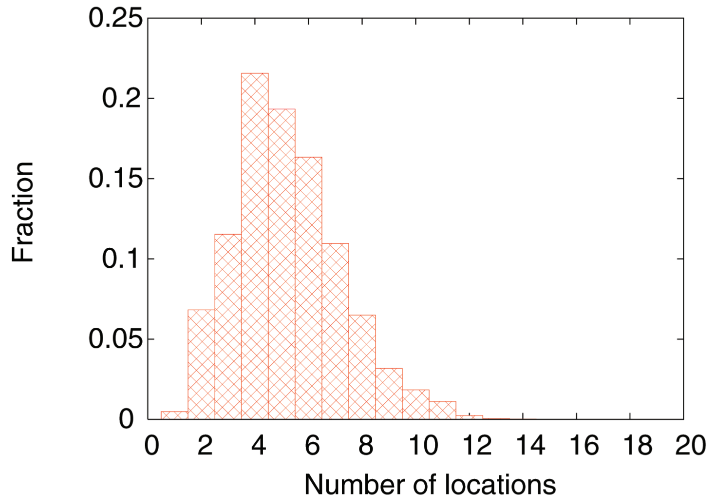

Fig. 1. Number of locations that a byte of domestic network traffic traverses in the national Internet infrastructure.

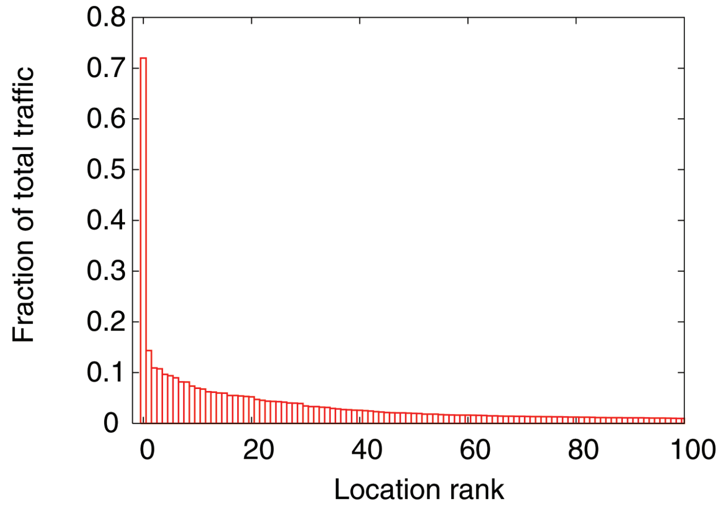

Fig. 2. Rank of Internet backbone locations based on the frequencies of their appearances on the path of each byte of domestic network traffic.

Funding Acknowledgments
Department of Homeland Security, National Infrastructure Simulation and Analysis Center